Atomic Energy Control Board
P.O. Box 1046
Ottawa, Canada
K1P 5S9

Commission de contrôle de l'énergie atomique
C.P. 1046
Ottawa, Canada
K1P 5S9

INFO-0220

RELIABILITY OF MICROCIRCUITS IN NUCLEAR POWER PLANTS

by

P.M. Cross and R.C. Taplin
Spar Aerospace Limited, RMSD
Weston, Ontario

A research report prepared for the
Atomic Energy Control Board
Ottawa, Canada

June 1986

Canada

Research report

RELIABILITY OF MICROCIRCUITS IN NUCLEAR POWER PLANTS

ABSTRACT

The reliability problems associated with modernizing control systems in nuclear power plants, particularly by using new technology microcircuits, are discussed and twelve problem areas identified. These are:

- new technology introduction;
- variability in manufacture;
- derating necessities;
- distributed systems;
- use of redundancy;
- electrostatic discharge damage;
- electromagnetic interference;
- nuclear radiation;
- thermal effects;
- contamination, including humidity;
- mechanical effects, including vibration; and
- testing.

Recommendations for the AECB are given in each area. Guidelines are given for the design, procurement, installation, operation and maintenance stages of use. Recommendations for further work are given.

RÉSUMÉ

Le présent rapport traite des problèmes de fiabilité liés à la modernisation des systèmes de commande dans les centrales nucléaires par l'utilisation de microcircuits de pointe et classe les problèmes en 12 catégories :

- l'introduction de nouvelles techniques de pointe;
- les variations dans la fabrication;
- la nécessité de sous-solliciter les composants;
- la décentralisation des systèmes;
- le recours au principe de redondance;
- les dommages dus aux décharges électrostatiques;
- les interférences électromagnétiques;
- les rayonnements nucléaires;
- les effets thermiques;
- la contamination, y compris l'humidité;
- les effets mécaniques, y compris les vibrations;
- les épreuves.

Les auteurs font des recommandations à la CCEA pour chaque catégorie. Ils fournissent des lignes directrices pour la conception, l'achat, l'installation, le fonctionnement et la maintenance comme étapes d'utilisation. Ils formulent enfin des recommandations sur le travail qui reste à faire.

DISCLAIMER

The Atomic Energy Control Board is not responsible for the accuracy of the statements made or opinions expressed in this publication and neither the Board nor the author assumes liability with respect to any damage or loss incurred as a result of the use made of the information contained in this publication.

TABLE OF CONTENTS

ABSTRACT		1
1.	INTRODUCTION	1
1.1	Purpose of the Report	1
1.2	Scope	1
1.3	General Background	1
1.4	Study Methodology	2
1.4.1	Overview	2
1.4.2	Collection of Relevant Information	2
1.4.3	Evaluation of Information	3
1.4.4	Preparation of Report	3
2.	FACTORS WHICH AFFECT THE RELIABILITY OF MICROCIRCUITS IN NUCLEAR POWER PLANTS	4
2.1	New Technology Introduction	4
2.2	Variability in Manufacture	5
2.2.1	Procurement Decisions	5
2.2.2	Use of the GIDEP System	8
2.2.3	Use of Screening	9
2.3	Derating Necessities	10
2.4	Distributed Systems	11
2.5	Redundancy	11
2.5.1	Use of Check and Switch Back-Up Systems	11
2.5.2	Use of Voting Systems	13
2.6	Electrostatic Discharge (ESD) and Surges	16
2.6.1	Background on ESD	16
2.6.2	The Present Situation in Ontario Hydro	21
2.6.3	Surges	21
2.7	Electromagnetic Interference (EMI)	22
2.8	Nuclear Radiation	23

TABLE OF CONTENTS (continued)

	2.9 Thermal Effects	25
	2.10 Contamination, Including Humidity	27
	2.11 Mechanical Effects, Including Vibration and Noise	28
	2.12 In-Service Testing	28
3.	GUIDELINES TO RELIABILITY ACTIVITIES AT THE LIFE-CYCLE STAGES OF MICROCIRCUITS	29
	3.1 Systems Design Decisions	29
	3.2 Design of Microcircuits and Microprocessors	31
	3.3 Procurement	31
	3.4 Installation	32
	3.5 Operation	32
4.	SUMMARY	33
	4.1 Collected Recommendations to AECB	33
	4.2 Summary of Recommendations Themes	36
	4.2.1 Priority Listing of Themes	36
	4.2.2 Recommendation for Urgent Action from Licensees	36
	4.2.3 Confidence in Reliability Figures	37
	4.2.4 Decision Rationales	37
	4.2.5 Survey Requests	37
	4.2.6 Future Work	37
5.	CONCLUSIONS	38
6.	DATA SOURCES AND REFERENCES	39

LIST OF FIGURES

FIGURE

1	The Normal Distribution	6
2	Triple Fully Redundant System With Voting	14
3	Triple Partially Redundant System With Voting	14
4	Triple Redundant Check and Switch System	15

LIST OF TABLES

TABLE

1	Generation of Static Electricity By Humans (Taken from DOD.HDBK263, 1980)	17
2	Classification of Electrostatic Discharge Sensitive Parts (Taken from DOD.HDBK263, 1980)	18
3	Sensitivities of Families of Semi-Conductors to Nuclear Radiation	24

1. SECTION I - INTRODUCTION

1.1 Purpose of the Report

The purpose of this report is to present guidelines for the design and use of microcircuits in nuclear power plants that will enable AECB to assure that the hardware reliability of control and shutdown systems is not eroded as forseeable changes in electronic technology are implemented.

1.2 Scope

This report considers the hardware reliability of Process and Special Safety (Shutdown) electronic control systems in CANDU nuclear power plants situated in North America, in the present and near-term future (five years). The procurement environment of other continents is not discussed. The instability in components manufacturer's business strategies and speed of innovation in electronics development makes the prediction of industrial electronics beyond five years futile; therefore speculation on longer term developments are avoided. It may be assumed, however, that trends of smaller size, lower power levels and greater sensitivities will be continued, while the intrinsic reliabilities of devices will rise.

Since the changes envisaged in many cases are changes in philosophy and system technology, the guidelines are necessarily wide in scope and do not attempt detailed instructions. Emphasis is laid on situations which are becoming more important in new technology, rather than areas which are well understood and to which design guidelines already apply.

1.3 General Background

The trend in CANDU nuclear power plant instrumentation and control is to move away from electromechanical systems into software systems situated in distributed microprocessors. The microprocessors themselves, and the larger central processors, are becoming smaller and running on lower power at higher temperatures. They are becoming swifter, more sensitive, cheaper and intrinsically more reliable than in the past. However, because of their speed, sensitivity, size and low power requirements they are more vulnerable to small changes in manufacturing process and operation environments. Due to the speed of introduction of new technology the history of the reliability of components and system is not as well characterised as in the past. When one adds that there is a significant economic incentive to situate the microprocessors in known hostile

environments such as generating halls or radiation containment areas, there is a potential for a serious hidden erosion in reliability.

In general procurement becomes a more important step than in the past in assuring reliability, and operating situations which in the past have been acceptable (electrostatic discharges, low electromagnetic field levels) may in the future be unacceptable.

1.4 Study Methodology

1.4.1 Overview

The work undertaken for this study was divided into three major activities:

(a) collection of relevant information
(b) evaluation of the information by appropriate specialists
(c) preparation of the report

The work was performed by a team of six from the Reliability group of Spar Aerospace Ltd., Remote Manipulator Systems Division, with extensive experience in very high reliability electronic systems. Many of the techniques used routinely within Spar are uncommon in other industries and the level of reliability achieved by these techniques may not be necessary for all nuclear applications. Nevertheless, the approaches to the problems should be similar and the concerns regularly analyzed by Spar should at least be visible to the Atomic Energy Control Board (AECB), especially with the increasing use of sensitive and sophisticated electronic control systems in CANDU plants.

1.4.2 Collection of Relevant Information

The needs of the AECB for information to help assess present and near future microcircuit applications were described in Appendix C of the Request for Proposal of this study. They were further clarified at the initial discussion meeting with AECB staff.

Information on present and projected plant environments both normal and after a Loss of Coolant Accident (LOCA) were obtained from the AECB through documents, meetings and telephone conversations. Information on present use of electronics and an indication of their reliabilities was also supplied to the Spar team via AECB documents.

Two of our electronic specialists, Mr. R. Taplin and Mr. F.J. Edwards, spent the morning of January 23rd touring the Pickering station and the afternoon touring the Darlington station, under the general guidance of the local senior AECB project officer. Their purpose was to gain a practical sense of the environmental conditions and to note situations of concern which might be invisible to residents of the stations.

Discussions with Ontario Hydro and Atomic Energy of Canada Ltd. designated contacts deepened our appreciation of the design approach of the licensees to reliability. While an extensive literature search was undertaken much of the information in this report was taken from the experience of the study team or internal Spar documents.

1.4.3 Evaluation of the Information

Regular meetings of the Spar team were held where the known properties and weaknesses of the candidate devices were discussed in relation to the CANDU environment. Issues of concern in procuring the microcircuit systems and in handling and protecting them during installation, operation and maintenance were reviewed in relationship to the significant safety aspects of the shutdown systems and the less stringent requirements of the process control systems. Design tradeoffs of reliability in microcircuits were laid out.

Conclusions were reached in the following areas:

(a) identification of factors existing in CANDU plants which reduce reliability by promoting device failure

(b) identification of factors in CANDU plants which reduce reliability by promoting device performance degradation

(c) identification of situations where confidence in the calculated reliability is reduced

(d) recommendations to AECB

(e) guidelines for designers and users

(f) suggestions for future work

1.4.4 Preparation of the Report

This report was prepared by the Project Manager, P. Cross, and reviewed by the

team members. In Section 2, factors which affect the performance and success of microcircuits are discussed individually and recommendations offered to the AECB, where the Spar team felt there was some present concern. In Section 3 guidelines are offered to be applied at various life cycle stages - design, procurement, installation, operation and maintenance. These guidelines are short and non-explanatory, the explanations being part of Section 2. Section 4 gives a summary of the report with a priority list of the recommendations to the AECB, including those for future work.

2. FACTORS WHICH AFFECT THE RELIABILITY OF MICROCIRCUITS IN NUCLEAR POWER PLANTS

2.1 New Technology Introduction

One general area of concern is the speed of innovation in the area of control systems. It is a truism in the reliability field that a known device with a lower, but established, reliability is to be preferred to one with a nominally higher reliability but with the possibility of great variation or without a complete history. It is the latter case that we are having forced on us increasingly. The new devices and systems have such great advantages, (low capital costs, lower running costs, faster and more accurate processing, nominally higher reliabilities) that it is easy to overlook the fact that the faster they are placed on the market, the less history we have of each. This is a difficult situation for the reliability engineer, who may not accept the unsubstantiated claims of the manufacturer when the safety of the public is at stake, and who has a responsibility to warn those in the use environment of operational and maintenance activities which may degrade the reliability.

To be more specific, the increasing use of digital microcircuits and custom software rather than electromechanical and analog devices for control is, theoretically, a good move from a reliability point of view, since less parts in general, and certainly less moving parts, immediately simplifies the system and as such increases its reliability. However, this gain can only be practically achieved if the weaknesses peculiar to new technology in general, and microcircuits and software in particular, can be identified and then eliminated by care in design, procurement, installation, operation and maintenance.

One disturbing weakness of modern digital microcircuits is their tendency to change state locally due to the presence of minor external transients (e.g., an electrostatic discharge, an electromagnetic field, nuclear or cosmic radiation etc). This change may not be seen as a failure, even with some error checking built-in. A piece of false data simply enters the decision making process.

(Since the mandate of this report is hardware reliability, no discussion will be given on the role of software in reducing the system reliability, but the attention of the AECB is drawn to its significance. It should be noted that predicting software reliability is a different activity from assuring its quality. Failure data should be presently being collected in preparation for its prediction).

Recommendation 1

(a) The AECB should indicate to its licensees that new technology not be adopted lightly. If adopted, an in-depth rationale showing very strong measures taken to assure reliability should be submitted to the AECB, with particular emphasis on procurement practices.

(b) As new microcircuit technology is adopted, the AECB should request assurance that those in the use environment are aware that their operational and maintenance activities will affect the reliability.

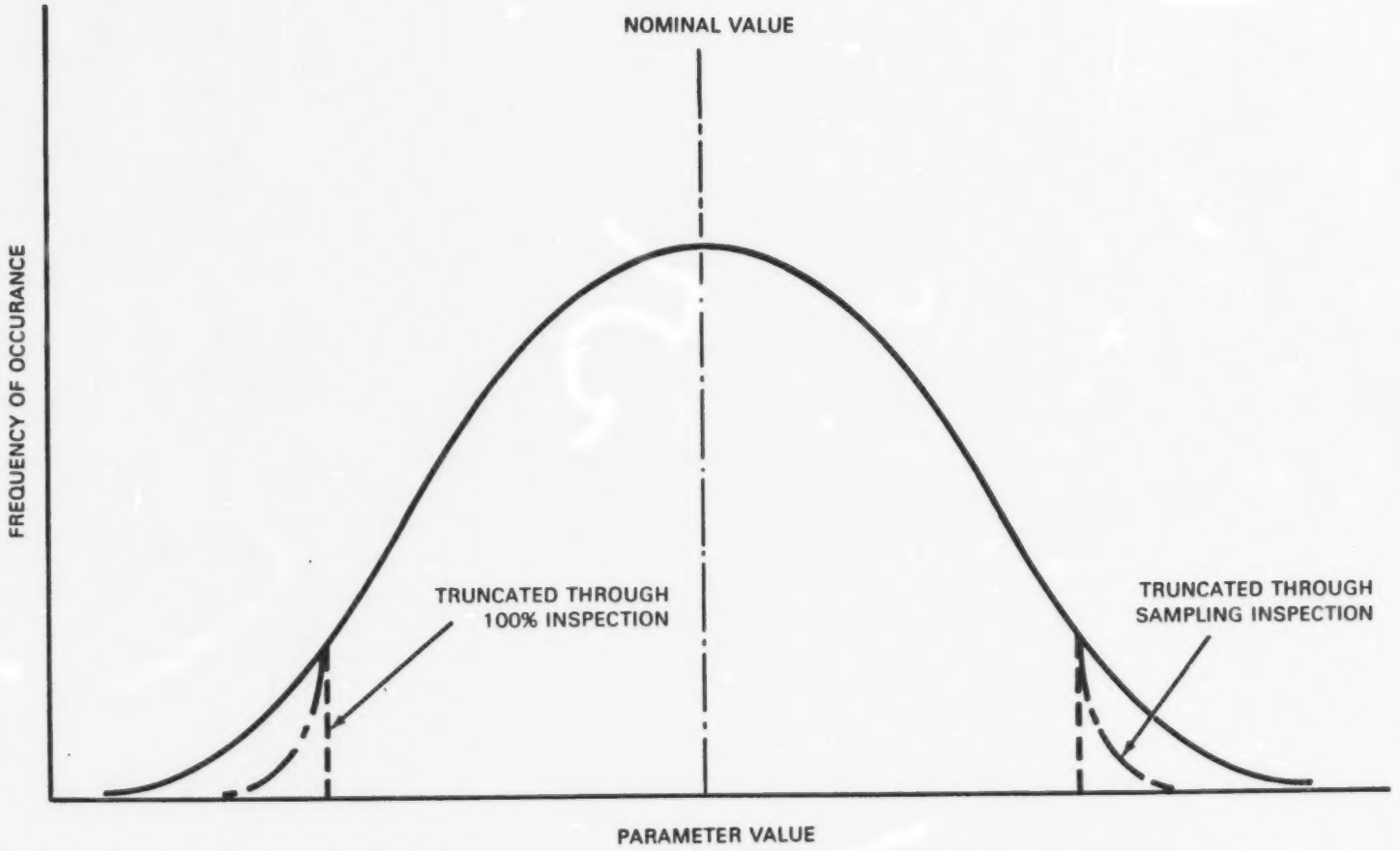
2.2 Variability In Manufacture

2.2.1 Procurement Decisions

The value of any parameter of a manufactured component cannot be considered to be identical within a batch of components. In general, as manufactured, the values will be spread over a Normal Distribution, as shown in Figure 1. By inspection and selection the batch offered for sale may be truncated by a more or less sharp step at one or both ends of the distribution.

The values quoted in the Manufacturer's catalog are maximum and/or minimum and, often typical values. These are obtained, of course, on a sampling basis. Unfortunately the variation in semi-conductor devices is often greater than that of other instrumentation and control devices due to the sensitivity of these devices to slight changes in manufacturing conditions.

While the manufacturers go to great lengths to control these conditions, nevertheless the variation device-to-device, manufacturer-to-manufacturer and even batch-to-batch, will itself vary; sometimes markedly. It should be of great concern to the user that properties of the batch actually being used, including reliability, may be outside the maximum/minimum ranges given in the catalog.



SPAR-P 988
ISSUE A

FIGURE 1 THE NORMAL DISTRIBUTION

Ways of increasing the confidence in the manufacturer's quoted reliability figures include:

(a) compiling one's own failure history of such devices,

(b) using the failure history of third parties who use a great number of these devices,

(c) auditing the manufacturing control

(d) relying on third parties auditing manufacturing control

While the compilation of failure history is expected to be a routine practice for the facilities under AECB licence, the volume of devices used is not great; hence, it is profitable to look at data from larger volume users. These may be industrial (e.g. GM, Westinghouse) or Military.

Some auditing of manufacturers is undertaken by the licensees under the Z299 procurement program, but it is rarely at the device or board level. In these circumstances it is wise to consider the merits of Military Standard (MIL-STD) parts.

These are parts whose properties, both nominal and the expected variation, are specified by one of the US Military Establishments. Manufacturers who wish to sell using this designation are physically audited by the Establishment at intervals and, after passing, are allowed on the Qualified Products Lists (QPLs). If a property is quoted as not less than a certain value for a Military Standard Part then one can have a higher confidence that the variation is sufficiently narrow to support this claim or that the distribution range has been narrowed by inspection and selection.

The production lines producing QPL parts are re-audited at intervals and extensive testing (Group C testing) is also conducted on selected batches from time to time. The result of this continual activity is that the QPLs are updated monthly.

In addition, the specified properties and the test methods used to measure them are in the public domain, being printed and available at a nominal charge from the US Military (Reference a). They are also available on microfilm from VSMF Data Control Services (Reference c) as are Canadian Military Standards and some Industrial and National Standards.

One aspect of this system is worth pointing out. It is common for many manufacturers to produce two versions of an electronic component, a MIL-STD part and 'Manufacturer's part number' part. The latter is usually quoted as being 'equivalent to MIL-STD X'. The Military parts are confined to certain production lines in certain plants. The QPL identifies the specific plants and lines qualified to make devices on the list. Since these are the only lines audited by the Military, it is fair to conclude that less stringent control may be kept on the other lines.

The engineer and the assembly manufacturer are wise to explain this situation to their internal procuring agent, since the statement 'equivalent to MIL-STD X' is often taken at face value by procuring agents and the (naturally) lower price of 'Manufacturer's part number' parts is attractive.

Recommendation 2(a)

The AECB should require that reliance not be placed completely on the manufacturer's catalogue value of reliability for devices but increased confidence be sought for critical systems by the use of MIL STD parts, parts endorsed by reputable third parties, in-house history of parts failure, or auditing or witnessing of the production by the licensees.

2.2.2 Use of the GIDEP System

One system which is useful to all designers and manufacturers of mechanical and electronic assemblies that require a high degree of reliability is the Government and Industry Data Exchange Program (GIDEP).

In this system various members of the industrial world pool information on technical matters in a relatively informal and timely fashion. One of the most important features of this system is a facility called 'Alerts'. When a problem has been found by a user in a class of products, this information is shared rapidly with all other users by the issuing of an Alert on the GIDEP System. The problem may be a generic problem, restricted to one manufacturer or even a class of products from one manufacturer over a limited period of time. In fairness to the manufacturers the staff of GIDEP require proof that the problem is a real one and it is usual for the reporting user to have discussed the problem with the manufacturer. The letters resulting will be published with the Alert. Often the manufacturer will offer suggestions on how to overcome the problem or will offer to recall the offending batches. In the case of direct safety problems this system is accelerated, but a normal problem may take about three weeks to be investigated and sent out. It is still faster and more effective than simple word of mouth.

Careful monitoring of the Alerts not only will allow avoidance of procuring devices with problems but also identifies devices in use which may need to be replaced or re-verified in order to maintain confidence in a reliable system.

About 6 Alerts on electronic devices are published each week so it is at least a part time job to monitor them continuously. An automatic electronic match of devices in CANDU instrumentation and control systems and devices with Alerts against them should be possible and this would significantly decrease the monitoring work.

Recommendation 2(b)

Discussions between the AECB and licenced facilities should be initiated on the joining of GIDEP and monitoring of its Alerts.

2.2.3 Use of Screening

Screening of microcircuits and other electronic devices is an activity which normally includes one or more 100% burn-in situations (elevating all devices to a high temperature for a protracted period) followed by one or more functional performance tests on all the devices. It may include the use of thermal cycling or thermal shock or other stresses as appropriate. The purpose of the activity is to cause failure of all devices with inherent weaknesses. The activity is extremely expensive, both for cost of burning-in and testing and also in loss of devices. However, confidence in the remaining components is considerably increased. Screening may be undertaken by the manufacturer as part of a military qualification program or as requested by the customer. It may also be undertaken by the customer either in-house or by contracting out to a neutral screening house. Screening may be supplemented by destructive physical analysis (DPA) of samples of lots to judge the acceptability of the lot or by 100% internal inspection of the circuits or devices at an early stage in their manufacture. (This inspection may be visual at the pre-cap stage of devices but may need to use a scanning electron microscope for the wafer stage of an integrated circuit). Visual and X-ray inspection of the finished product may also be specified as part of the screening process. JAN MIL.M.38510 integrated circuits which have been screened to MIL STD.883 Method 5004 and military approved will carry the letters C, B or S to indicate successively tighter levels of screening. The price rises by approximately a factor of 6 for each level. Screened military approved semiconductor transistors and diodes are identified as JAN, JANTX, JANTXV and JANS to denote successively tighter levels of screening. Electrical parts (e.g., relays, coils, connectors, etc.) may be purchased to Established Reliability, (ER) Grades L through T. Commercial grade, military grade and military ER and JAN grade parts are generally physically and functionally interchangeable with the basic difference being the failure rate levels, which can vary in the order of magnitudes.

Screening has been used on some Ontario Hydro equipment but is uncommon. In a CANDU environment screening may be considered when:

(a) the variability of performance of a type of device is known to be high

(b) new technology is to be used where variability of manufacture is unknown;

(c) the reliability of the part is critical;

(d) stresses common to several redundant devices are predicted (e.g., radiation after a LOCA).

No specific recommendation on screening is offered in this report, but its use is discussed in several of the following paragraphs.

2.3 Derating Necessities

While a device may be certified to withstand certain stresses, the stresses nevertheless do, marginally but cumulatively, degrade the performance and expected life of the device. For this reason it is common practice to select devices such that they see only part of the stress for which they are rated; this is known as derating. The types of stress derating may include power, voltage , temperature and radiation. It is common to derate to 75% or 50% of the certified rating but Hughes Aircraft, for example, allows only 10% of the certified rating of critical items as a design limit for the environment. The negative effects of stress are increased as more types of stress are involved, often in a non-linear manner. Under no circumstances should the certified limits of stress be designed to be approached simultaneously for two or more types of stress for a device.

Since we may expect even a stress derated component to degrade over time, it is wise to derate the performance characteristics as well as the stress factors, that is, to choose a device whose validated known limits are significantly higher than needed at the beginning of the device life time. The performance trends on critical items also need to be evaluated from time to time.

Recommendation 3

(a) The AECB should request the derating rationale as part of the reliability estimates.

(b) The AECB should request a list of critical electronic components expected to degrade with age to be drawn up, and a plan for in-service tests to track their performance changes be developed.

2.4 Distributed Systems

At the present time most control and shutdown systems licenced by AECB are centralized, that is, detection devices are spread over wide areas in the nuclear power plants and they send electric signals back to a centralized processing room where the signals are processed on mini computers and the action signals sent to the electromechanical control devices. From a reliability point of view the elements in the most hostile environments are the detectors, cabling and control devices and, except for special circumstances, one would only expect to lose those one at a time. While the centralized processing system is vulnerable to failure affecting all of the signals at one time, it is less likely to do that in its protected atmosphere. The disadvantages of this system are mainly the cost and inconvenience of the amount of individual long distance cables. In addition the detection devices are getting harder to buy alone without built-in processors. This may force a move to distributed systems.

In the distributed system the processing is initiated at the detection site, signals are multiplexed to a central site for visibility and/or action. The amount of multiplexing cable needed is much less than individual cabling and, as such, is cheaper, more convenient and easier to protect.

How the reliability is affected depends upon the signal rate from the distributed microprocessors to the centralized processor and the (electrical) noise the cable will bear. If the microprocessors have significantly reduced the amount of information needed to be sent to the centralized processor the signal rate along the multiplexed line may not be much greater than that along the individual cables in the older system. This will imply that the electrical noise protection offered these cables will be good enough for the multiplexed cable. If however a considerably higher rate is required more care will be required to protect the cable against electromagnetic interference, surges, electrostatic discharge and mechanical damage.

Recommendation 4

The AECB should expect the level of physical and electrical noise protection given to cable carrying multiplexed signals to be explicitly matched to the planned baud rate.

2.5 Redundancy

2.5.1 Use of Check and Switch Back-Up Systems

One standard method of increasing the reliability of whole systems, or critical

parts of a system, is to introduce one or more back-up systems to run in parallel with the critical system and take over in a case of a primary failure. For a singly redundant system the reliability is doubled by this method and for double redundancy it is tripled, assuming no common mode failure, and that back-up systems are on standby rather than running operational. However, if the reliability of the single system is low, tripling it may still not raise the overall reliability to an acceptable level. This is a particular concern if the reliability of the system is unknown. If, for example, components are purchased in a local market where reliability figures are unknown or the quoted figures are suspect, then the practice of redundancy does not automatically eliminate the doubt of safety. As we discussed in Paragraph 2.1, these situations may arise even in North American markets and can be expected to become usual as new technologies without local histories become more and more common.

When a reliability analysis is undertaken it should be taken to the lowest level of procured components. The reliability of procured components should, in theory, be demonstrated by the vendor. However, it is not uncommon for the vendors to be unable to develop this information. In this case either the licensee should perform the analysis itself or confidence in the component should be generated by a number of apparently satisfied customers. This is particularly true with commercial microprocessors.

Recommendation 5(a)

The use of redundancy should not be allowed to obscure safety concerns over components with low or unknown reliabilities. Efforts should be made to ensure procurement of components whose reliability is known and which enjoy a high degree of confidence.

There are two other situations which weaken the confidence in a system with redundancy. One is that the back-up systems may become inoperative between installation and needed use (a broken connection due to vibration for instance). The other is that not all primary failures are announced, so that the back-up system may be running without the knowledge of the operator. In both these cases the reliability the system is cut to one-half (or two-thirds for double redundancy) and maintenance may not be initiated. In-service testing and annunciation of failures for all parts of the system, especially standby systems, overcomes this in part. The frequency of testing depends upon the criticality of system.

Recommendation 5(b)

Frequent software-initiated built-in tests (BIT) with failure display should be considered for all standby subsystems and parts whose failures will not be announced.

2.5.2 Use of Voting Systems

With processing systems it is common for all of the redundant parts to run continuously and for them to compare results from time to time, voting on the outcome. This may be more economical than the check and switch system because it should allow the automatic use of correct data and failure detection without external testing. However, the stage at which voting takes place needs to be considered carefully if more than one failure in all the systems are to be guarded against.

For example, consider a simple triple redundant sensor-processor system voting at the inputs of each processor, and voting on the outputs of all three processors together. Figure 2 shows the situation with one failed sensor and one failed processor. The decision is made correctly. It is not uncommon presently for sensors and processors to be bundled together in a black box, that is, to have a single connection between each sensor and a specific processor. It is clear that for a correct decision in such a partially redundant system where voting only takes place between all the processors at the output of the processors, one would need five sensor/processor sets if there were two failures and the voting were implemented naively (see Figure 3 for triple partially redundant case). The situation can be improved if the processors are linked together by a Byzantine Agreement protocol. This is a protocol which constrains all non-failed processors, to agree on the (binary) output signal and also constrains the output signal to be the same as the input signal. The computation proceeds by the sending and receiving of messages in a series of rounds over a network that is fully connected and reliable. Part of the computation requires generating random coin tosses. It can be shown that for 't' expected failures, one will require at least 3t+1 processors to be able to implement a Byzantine Agreement protocol. The algorithms for achieving this agreement are still being researched. In the case discussed since only one processor has failed, the correct agreement can be reached by four processors.

It should be noted that if external testing is used to diagnose failures and the process switched to a failure-free system, only three systems would be needed for a correct decision (Figure 4). This discussion shows clearly that while voting appears to save external or internal testing it increases the amount of hardware necessary and introduces sophisticated complications to the system. The area of confidence in the results of voting systems subject to faults is an extremely complex one and warrants further study by the AECB.

Recommendation 5(c)

The AECB should ensure that the logic of the reliability of advanced technology voting systems is demonstrated by design groups.

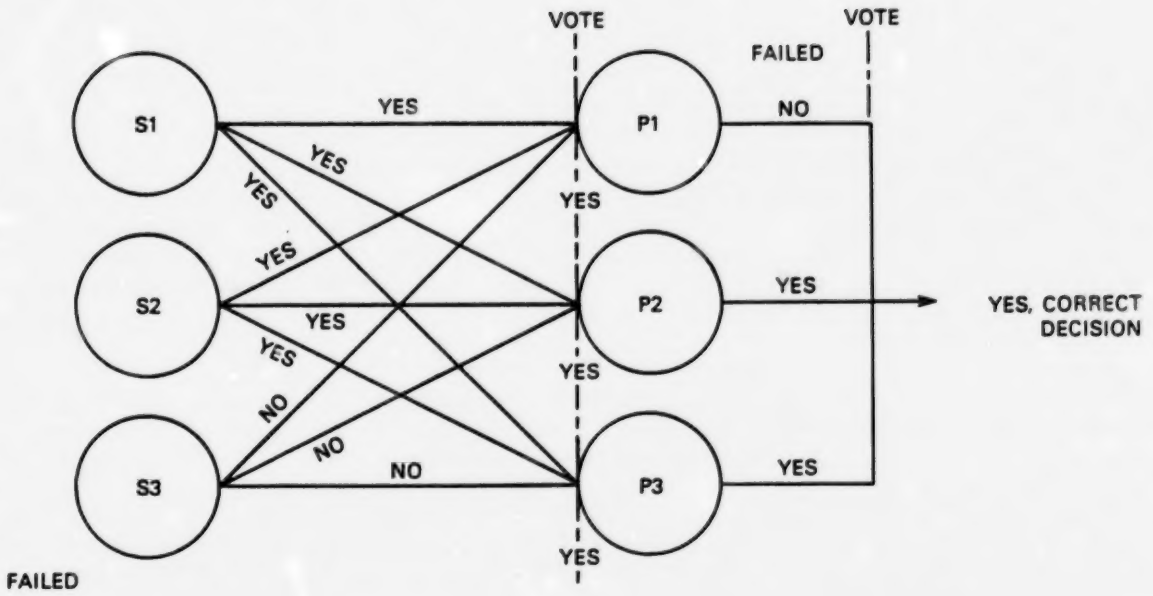


FIGURE 2 TRIPLE FULLY REDUNDANT SYSTEM WITH VOTING

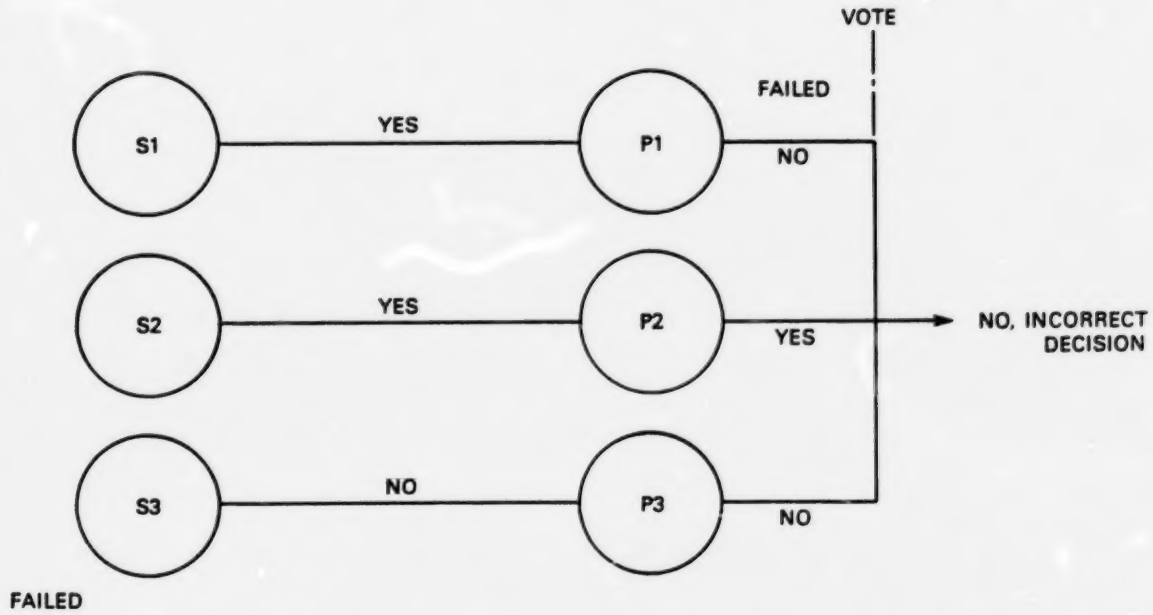


FIGURE 3 TRIPLE PARTIALLY REDUNDANT SYSTEM WITH VOTING

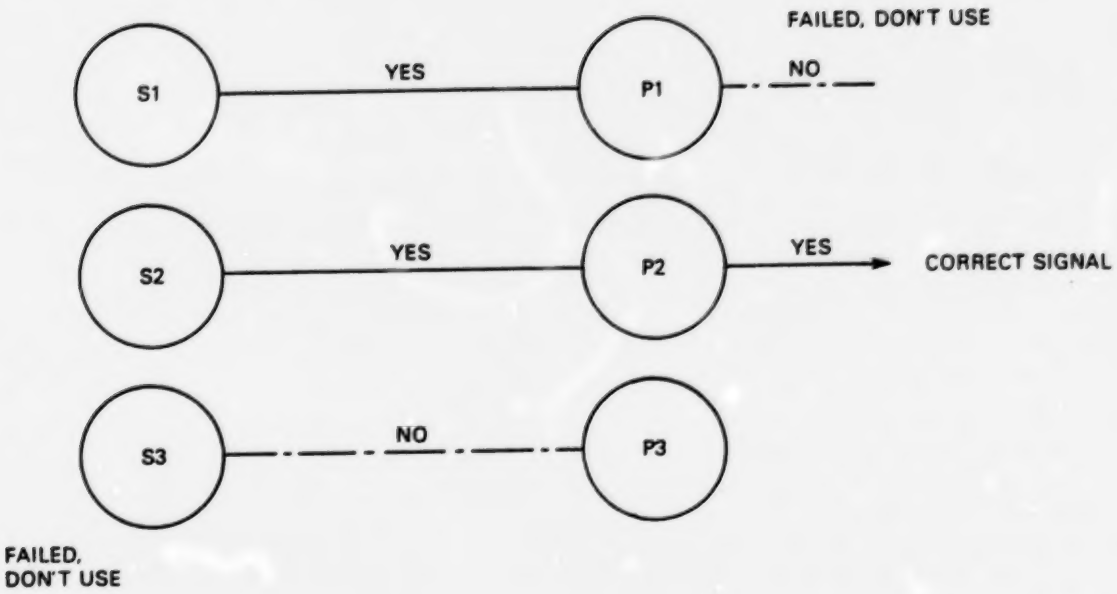


FIGURE 4 TRIPLE REDUNDANT CHECK AND SWITCH SYSTEM

2.6 Electrostatic Discharge (ESD) and Surges

2.6.1 Background on ESD

When two unlike substances are separated, an electrostatic charge is left on one surface and the same charge but with opposite polarity on the other. When the surfaces are conductive this charge leaks quickly away to ground but for non-conductive surfaces the charge remains and may build up with repeated separations until it reaches the breakdown voltage of air when it will arc across to the nearest ground.

Under the normal rather low humidity conditions indoors in Canada, humans pick up high electrostatic charges as they move about, especially when the environment has a large portion of insulating synthetics in it. These charges will move quickly across any more-conductive surfaces and while they usually have a low charge density, the voltage difference between the person and ground may be very high. For typical voltage differences generated see Table 1. This energy discharge is capable of damaging many electronic devices, especially low signal integrated circuits. The more advanced devices are particularly susceptible to electrostatic discharge (ESD) and the trend is becoming more pronounced (See Table 2).

It is common to protect such sensitive devices with an input suppressor of some type; but it should not be imagined that the installation of a suppressor solves the problem. The protective device only reduces the voltage seen by the sensitive component and may not have a fast enough reaction for very short spikes. Worse, the effort of ESD is not always catastrophic; often there are simply transient effects or a decrease of performance which may not be detected by built-in tests or even unskilled human testers. This effect, as with other reliability degradations, may lead to false data on which safety or other decisions are made.

ESD has been found to cause the following failures in integrated circuits:

- o intermittent or transient failure (ghost bytes, malfunctions)
- o breakdown of insulation
- o latent failure; the degradation of the devices occurs later than the ESD is seen. The failures may not be understood to be caused by ESD.

ESD affects other devices in a similar manner; magnetic tape problems and noise interrupts are also attributable to this situation.

Table 1: Generating Static Electricity

by Humans (taken from DOD.HDBK 263, 1980)

Means of Static Generation	Electrostatic Voltages	
	10 to 20 Percent Relative Humidity	65 to 90 Percent Relative Humidity
Walking across carpet	35,000	1,500
Walking over vinyl floor	12,000	250
Worker at bench	6,000	100
Vinyl envelopes for work instructions	7,000	600
Common poly bag picked up from bench	20,000	1,200
Work chair padded with polyurethane foam	18,000	1,500

TABLE 2: Classification of Electrostatic Discharge Sensitive Parts

(taken from DOD.HDBK 263, 1980)

CLASS 1: SENSITIVITY RANGE 0 TO ≤1000 VOLTS
• Metal Oxide Semiconductor (MOS) devices including C, D, N, P, V and other MOS technology without protective circuitry, or protective circuitry having Class 1 sensitivity
• Surface Acoustic Wave (SAW) devices
• Operational Amplifiers (OP AMP) with unprotected MOS capacitors
• Junction Field Effect Transistors (JFETs) (Ref.: Similarity to MIL-STD-701: Junction field effect, transistors and junction field effect transistors, dual unitized)
• Silicon Controlled Rectifiers (SCRs) with Io<0.175 amperes at 100° Celsius (°C) ambient temperature (Ref.: Similiarity to MIL-STD-701: Thyristors (silicon controlled rectifiers))
• Precision Voltage Regulator Microcircuits: Line or Load Voltage Regulation <0.5 percent
• Microwave and Ultra-High Frequency Semiconductors and Microcircuits: Frequency >1 gigahertz
• Thin Film Resistors (Type RN) with tolerance of ≤ 0.1 percent;power >0.05 watt
• Thin Film Resistors (Type RN) with tolerance of > 0.1 percent;power ≤0.05 watt
• Large Scale Integrated (LSI) Microcircuits including microprocessors and memories without protective circuitry, or protective circuitry having Class 1 sensitivity (Note: LSI devices usually have two to three layers of circuitry with metallization crossovers and small geometry active elements)
• Hybrids utilizing Class 1 parts
CLASS 2: SENSITIVITY RANGE >1000 TO ≤4000 VOLTS
• MOS devices or devices containing MOS constituents including C, D, N, P, V, or other MOS technology with protective circuitry having Class 2 sensitivity
• Schottky diodes (Ref.: Similiarity to MIL-STD-701: Silicon switching diodes (listed in order of increasing trr))
• Precision Resistor Networks (Type RZ)
• High Speed Emitter Coupled Logic (ECL) Microcircuits with propagation delay ≤1 nanosecond
• Transistor-Transistor Logic (TTL) Microcircuits (Schottky, low power, high speed, and standard)
• Operational Amplifiers (OP AMP) with MOS capacitors with protective circuitry having Class 2 sensitivity
• LSI with input protection having Class 2 sensitivity
• Hybrids utilizing Class 2 parts

Table 2 (Cont'd.): Classification of Electrostatic Discharge Sensitive Parts

CLASS 3: SENSITIVITY RANGE >4000 TO ≤15,000 VOLTS
• Lower Power Chopper Resistors (Ref.: Similarity to MIL-STD-701: Silicon Low Power Chopper Transistors)
• Resistor Chips
• Small Signal Diodes with power ≤ 1 watt excluding Zeners (Ref.: Similarity to MIL-STD-701: Silicon Switching Diodes (listed in order of increasing trr))
• General Purpose Silicon Rectifier Diodes and Fast Recovery Diodes (Ref.: Similarity to MIL-STD-701: Silicon Axial Lead Power Rectifiers, Silicon Power Diodes (listed in order of maximum DC output current), Fast Recovery Diodes (listed in order of trr))
• Low Power Silicon Transistors with power ≤5 watts at 25°C (Ref.: Similarity to MIL-STD-701: Silicon Switching Diodes (listed in order of increasing trr), Thyristors (bi-directional triodes), Silicon PNP Low-Power Transistors (Pc ≤5 watts @T_A = 25°C), Silicon RF Transistors)
• All other Microcircuits not included in Class 1 or Class 2
• Piezoelectric Crystals
• Hybrids utilizing Class 3 parts

The area of ESD damage and its control is a complex one. In this respect we merely make the problem and an outline of its solution visible to the AECB.

In addition to protective circuits, ESD sensitive devices need to be handled with the greatest care and with as much grounding for the personnel and devices as possible. The following products should be considered where such devices are to be handled.

(a) Grounded wrist straps
(b) Conductive, grounded table tops
(c) Static-protective bags and boxes for transportation
(d) Static-protective smocks
(e) Conductive, grounded floor mats

The packaging materials in which such devices are delivered (as spares for example) from the manufacturers may be expected to be static protective. It is imperative to follow to the letter any instructions on withdrawing and unwrapping the devices from the packaging and subsequent handling. If these are not followed the withdrawal itself may set-up a damaging electrostatic charge on the device.

Perhaps the most important parts of any ESD control systems are the training and motivational programs for the personnel involved with ESD sensitive parts.

The ESD problem is a serious one now and growing more difficult as we look to smaller and faster semiconductor products. The very impetus which suggested this study will surely recognize the need for present work and future planning to control ESD. Today's silicon based CMOS, HFET AND VSLI-HMOS devices can be seriously affected by less than 100 volts of static electricity. As an example of future trends consider the use of gallium arsenide semi-conductor devices. GaAs devices are able to handle analog as well as digital signals. They can emit light and also process electronic data, making them ideal for telecommunications and local area networks (LANS). Memory capacities are improved significantly with three to six times the processing speeds of silicon devices. Lower power requirements and higher operating-temperature capacities open the way for further equipment advances and miniaturization. It would seem that, assuming no technological barrier, we will move to GaAs devices on a routine basis relatively quickly. However, the GaAs semi-conductor devices are <u>five times</u> more static sensitive than CMOS devices. Trying to protect these devices, singly or while board mounted, from exposure to 20 volts of static electricity will be a formidable task.

2.6.2 The Present Situation in Ontario Hydro

During the tours of the Ontario Hydro plants at Pickering and Darlington, Spar team members noted that while staff engineers knew of the need for care with ESD devices, there was no evidence of protective devices for personnel or of reminder posters or warnings about how to handle such products in the control equipment rooms or the repair area. There does not appear to be a formal ESD training program for those who test and maintain systems containing these devices. It is likely that this situation is the same at other facilities as the extent of the danger of ESD to modern microcircuits has only been generally understood recently.

In the few parts lists we reviewed for this study we found, as we expected, that static sensitive devices are presently being used in Ontario Hydro Systems. The parts list for the Fisher Porter 50KM2000 Chameleon Process Controller, Main Board, identifies seven ICs as static-sensitive. In the parts list of the OH 180 Programmable Controller, at least 3 parts are clearly the type that would be expected to be sensitive, although they are not so identified.

Recommendation 6

(a) The AECB should request a full ESD control plan from its licensees. The Plan should stress the occurrence of transient effects and latent failures as well as direct failures.

(b) The AECB should investigate this area in more depth with all deliberate haste.

2.6.3 Surges

The current and voltage supplied to the equipment is expected to vary from the nominal over time. Relatively frequently, sudden increases or decreases may be expected, and are known as surges. Unprotected, most microcircuits would be damaged by these surges; hence, it is normal to place regulators at the input of most black boxes and to add surge suppressors; (e.g., movistors) near particularly sensitive devices, such as microcircuits. One aspect of this protection which does not appear to be part of the CANDU reliability philosophy is that the suppressors are themselves damaged by the surges and increasingly pass on the burden to the "protected" components.

The life time of the suppressors, or the suppressor-device pair, can be estimated in conjunction with the manufacturer of the suppressor.

Recommendation 6(C)

The AECB should request expected life-times of devices sensitive to and subjected to surges, even when they are protected by suppressors.

2.7 Electromagnetic Interference (EMI)

The movement of electric current is always accompanied by changes in the electromagnetic field around it. These changes may cause the movement of current in another conductor within the field. In many cases spurious currents are set up in an undetermined manner in conductors, and in microcircuits, especially digital ones, electromagnetic interference (EMI) may cause false signals and data to be passed on to the decision making stage. Because these effects are often transient they may not be seen as 'failures' of devices and even if they are, trouble shooting and solving the problem will be complex.

Preventative measures at the design and operation stages should be taken to reduce the problem.

Certain device configurations act as excellent EM emitters and receptors; in microprocessors these include:

- clocks
- logic gates
- printed circuit board traces

The problem they pose as radiators is affected by the current flowing, the loop area it is flowing in and, in the case of logic gates, the logic gate bandwidth. Interestingly, for this situation, CMOS logic is preferable to other logic families because it has a lower bandwidth and smaller currents.

Design solutions to reducing the electromagnetic fields radiated from microprocessors include careful selection of devices and lay-out of boards (reduced loop areas).

The problem they pose as receptors is affected by the 'noise margin'; the bandwidth and length of interconnects. (The noise margin is the minimum noise amplitude on an input that results in an output state transition). The greater the noise margin and the larger the bandwidth, the better the immunity to pick up. Again the problems can be reduced by choice of devices and layout.

Once the printed circuit board has been optimised for minimal EMI, residual interference can be further reduced if the board is placed in a shielded

enclosure and care taken with the openings into the enclosure. Other aspects of EMI fall under general coupling considerations and do not fall within the mandate of this report.

Recommendation 7

(a) The AECB should require the designers to demonstrate that EM emission and EMI immunity have been formally considered in the design of custom processors at board and/or system levels as well as normal coupling EMI considerations.

(b) Surveys of typical EM fields should be conducted in the types of areas under new consideration for situating electronic systems (e.g., generating halls, containment areas).

2.8 Nuclear Radiation

Nuclear radiation which affects electronic systems is considered under two headings, neutron flux and ionizing radiation. The first has a bulk effect and as a result the cumulative result of radiation is of most interest. The second has a mainly surface effect so transient as well as cumulative effects are important.

Presently there are little or no electronics in containment areas and few in working generating halls. However, some planning for the future sees a rapid dissemination of processors in the generating halls and even in the containment areas. In general it may be assumed that there are no radiation effects in the generating halls. Information on expected radiation within the containment area was, surprisingly, hard to obtain. The Safety Systems Engineering Design Guide (Qualifying Safety Related Electrical &Instrumentation and Control Equipment for Environmental Service Conditions) for Point Lepreau (DG.87.68000.3) published in 1975 gives only the temperature and humidity for normal and accident conditions, while the equivalent document for Pickering B (DG.30.68000-3) Rev. 2 published in 1980 also gives expected radiation rate for ionizing radiation in normal conditions and the accumulated radiation doze during six months following a LOCA accident. No expected transients are given (as they are for temperature) and it is specifically stated that "the effect of LOCA radiation dose should only be considered in conjunction with the long term test". The normal radiation is expected to be 10 Rads/hr in general and up to 100 Rads/hr in the Feeder Cabinet. The post-LOCA accumulated dose is given as 10^7 Rads. The neutron flux is expected to be low in-service and even lower after an accident. A typical table of sensitivities to radiation of families of semiconductor devices is given in Table 3. For normal service 10 rads/hr leads to approximately 10^5 rad total dose over one year. Most of the devices from the semiconductor families of

TABLE 3

SENSITIVITIES OF FAMILIES OF SEMI-CONDUCTORS TO NUCLEAR RADIATION (from Electronics, March 16, 1978; p.131)
(rads[Si] stands for roentgens absorbed dose in silicon)

RADIATION ENVIRONMENT \ SEMICONDUCTOR TECHNOLOGY		DISCRETE BI-POLAR TRANSISTORS AND J-FETs	SILICON CONTROLLED RECTIFIERS	TTL	LOW POWER SCHOTTKY TTL	ANALOG INTEGRATED CIRCUITS	C-MOS	n-MOS	LIGHT EMITTING DIODES	ISOPLANAR II ECL
NEUTRONS (n/cm^2)		10^{10}-10^{12}	10^{10}-10^{12}	10^{14}	10^{14}	10^{13}	10^{15}	10^{15}	10^{13}	$>10^{15}$
IONIZING RADIATION	Total Dose (rads[Si])	$>10^4$	10^4	10^6	10^6	5×10^4 -10^5	10^3-10^4	10^3	$>10^5$	10^7
	Transient Dose Rate (rads[Si]/s) (Upset or Saturation)	---	10^3	10^7	5×10^7	10^6	10^7	10^5	---	$>10^8$
	Transient Dose Rate (rads[Si]/s) (Survival)	10^{10}	10^{10}	$>10^{10}$	$>10^{10}$	$>10^{10}$	10^9	10^{10}	$>10^{10}$	10^{11}
	Dormant Total Dose (Zero Bias)	$>10^4$	10^4	10^6	10^6	10^5	10^6	10^4	$>10^5$	$>10^7$

Table 3 would fail within one or two years without shielding. Methods of shielding systems from radiation are not discussed in this report, as the expertise is expected to be high within the AECB and the licensees' establishments.

Without the information on short (<1 sec) bursts of ionizing radiation that may be expected just after an accident, no conclusions as to the performance, or even the survival, of these devices, shielded or unshielded, after an accident can be drawn. The conservative assumption must be that they are lost. If information signals are needed from this area after an accident, as we assume they are, the detector should be hardwired out to electronics outside the area in addition to having the signal processed within the area. (Most detectors will themselves be robust enough to survive LOCA radiation conditions). If the radiation profiles after a LOCA were known, radiation hardened devices would be needed, even with shielding.

Radiation hardened microcircuits are designed to be able to withstand specified levels of radiation. The confidence that this has been achieved is gained by sampling the devices at the wafer stage, with destructive radiation testing of the sample. This is sometimes known as screening but it should be noted that screening normally implies 100% stressing and testing, whereas in this case only samples are taken.

Recommendation 8

(a) The AECB should pursue, via licensees or on its own initiative, development of a model or analysis of other accident data to allow prediction of local radiation changes both in space and time immediately after a LOCA.

(b) Until this information is available, licensees should use the assumption that all electronic devices in the containment area are failed immediately after a LOCA.

2.9 Thermal Effects

Heat is a stressor for microcircuits, it may degrade the performance and cause latent faults in the devices to assume importance and cause failure. The types of faults uncovered will vary depending on the temperature imposed, the time duration, the rate at which it is applied (shock effects) and cycling. It is these effects which are deliberately imposed in a screening system to force early failures. Even using screened lots, heat will accelerate the aging, and derating should always be applied to temperature limits. Devices taken from unscreened lots may be particularly susceptible to the effects of heat; derating and careful control of the environment is necessary for reliable usage. (In passing it is noted that all electronic parts are susceptible to heat. For

example, few capacitors can survive more than 85°C even for a short period.)

At the moment most microcircuits in CANDU plants are situated in control equipment rooms where air conditioning is an integral part of the safety system and appropriately backed up. However, it is proposed that microprocessors be distributed in the generating halls and even in the containment area. In both cases temperatures vary widely over space and time even in normal circumstances. The choice of where to situate microprocessors and the supplemental cooling needed is a serious concern. Clearly they should not be located near any thermal sources such as cooling baffles from other equipment or steam pipes and boilers, even if these are insulated. (This is to guard against accident conditions or maintenance conditions when the insulation is removed.) It should be noted too that the temperature inside louvered cabinets will inevitably, because of heat production by the equipment, be higher than in the general environment, by perhaps as much as 30°C. The problem will be accentuated in a closed water-proof environment and local cooling may be necessary.

When the allowable temperature limits of the environment are considered, the derated limit should be used by the designer and not the manufacturer's specification limit. The latter limit may be used as the absolute worst case accident limit. Commercial devices normally have a manufacturer's upper specification of 70°C. Derated (for example) to 40°C, this implies very careful cooling control of distributed microprocessors in enclosures in an ambient generating hall temperature of 25°C. Ideally, even when distributed, the microprocessors should be gathered together in groups in a protected and temperature controlled environment. This theme will be re-iterated in Paragraph 2.10.

For microprocessors in the containment area the same general statements apply. However, the very significant temperature swings after a LOCA demand special attention. In Recommendation 8b) we suggested that, at least until the true radiation profiles after a LOCA are available, it is assumed that all electronic devices in the containment area are lost immediately after a LOCA. To that we would add now that relaxation of that rule would require that the microprocessors be analysed for their expected reaction to the severe thermal cycling expected.

Recommendation 9

(a) The AECB should express a preference to licensees that distributed microprocessors be grouped together in clean, protected, water-proof, temperature controlled, humidity controlled areas away from main thermal sources, or in cooled enclosures.

Where this is not possible the microcircuits and devices should be enclosed and specified to higher temperatures; consideration may be given to using screened components in order to have confidence in stated reliabilities with uncertain environments.

(b) The AECB should request thermal profiles of locations in which retrofit microprocessors are to be situated.

2.10 Contamination, Including Humidity

Many contaminants affect microcircuits negatively, the major effects being:

(a) production of unwanted conductive paths
(b) production of unwanted insulative paths
(c) corrosion or breakdown of existing paths and insulators.

The most important contaminant which gives the first effect is water, in liquid or gaseous (humidity) form. The concern over deluge with water has been identified in the past by the AECB. For example, the Environment Qualification of Safety Related Equipment for both Point Lepreau and Pickering B states that steps are to be taken to minimise the risk of water, spray and steam. Suggestions are to use waterproof enclosures or totally enclosed and protected areas to locate the devices suitably. In the latter case humidity may still be a problem. The design specifications for inside and outside the containment area is up to 95% humidity. For the smaller circuits in increasing use today, humidity poses a true problem in the way it did not in the past. The only solution is protection and the attention is drawn to Recommendation 9a.

Other, probable conductive contaminants are metal particles (e.g., stranded wire fragments) and carbon from brushes. Typical insulative contaminants are dust, sand, etc. While it is felt that adequate precautions are presently taken during operation, attention is drawn to specific situations during maintenance. Open items which are not being worked on, must be covered by dust covers. This includes decoupled connectors away from the maintenance site. Clean work surfaces for repair should be maintained at all times.

Corrosive or breakdown agents include moisture, acids, alkalis, fungus and other biological agents. Less obvious agents are lubricants, including hydraulic fluids and cleaners, especially printed circuit board cleaners. For example, aluminum capacitors are particularly susceptible in damage from printed circuit board cleaners. Workmanship standards of removing all cleaners, and coating the boards with resistant finishes, and also using material standards to provide insulators which are resistant to common lubricants and cleaners are necessary.

Recommendation 10

The AECB should request that directives for repair areas emphasise the danger to microcircuits of debris from repair activities and of contaminants, including common cleaners.

2.11 Mechanical Effects, Including Vibration and Noise

On the whole, steady state mechanical stresses, whether tension, compression or pressure, do not cause failures in microcircuits except through gross cracking. This is in general true for seismic effects also. Shock, however, may cause undetected internal cracking. Vibration, even in the acoustic range, may loosen smaller connections, especially the solder joints, and cause failure. It should be noted that a black box on a vibration table may apparently not resonate at acoustic frequencies but that airborne acoustic pressures may damage small components and connections anyway. That is, formal vibration testing may not uncover deleterious effects due to airborne noise. In general, a noticeably noisy environment may indicate a threat to the integrity of electronic assemblies. Acoustic induced vibration may be considered a potential stressor of microcircuits in the generating halls. Electronic equipment which is to be situated there or in other noisy areas needs stress-relief techniques to be specified as part of the design and may also, depending on the severity of the environment, require vibration mounting or damping.

Recommendation 11

(a) The AECB should request that for locations with expected high amplitudes of sonic or subsonic vibrations (i.e. noisy areas), the protection of all microprocessors be explicitly demonstrated by the licensees.

(c) The AECB should request vibratory profiles of locations in which retrofit microprocessors are to be situated.

2.12 In-Service Testing

Testing, whether routine as part of preventative maintenance or ad hoc as part of a fault finding exercise, is inevitable in the operation of instrumentation and control systems. The testing may be automatic and internal (built-in test or BIT) or the stimuli may be applied by human intervention and the results interpreted by humans. While BIT offers the advantage of labour saving (and thus allows more frequent testing), in either case non-expert testers may misinterpret patterns of results, especially those signalling partial failure. Expert human testers should be used where patterns are non-standard. In the

future one might hope software expert systems may also be implemented to allow BIT sensitivity to compliant but non-standard test results. For the present, care must be taken to structure the type, sequence and severity of testing so as to avoid degrading the system by the action of testing itself. With microcircuits' sensitivity and speed of reaction this is becoming a greater problem than in the past.

It should be noted that a particularly dangerous time for a reactor system is when maintenance is being undertaken (e.g. the recent accident at Chernobyl). Since the detection and corrective action system is heavily dependent on microcircuits it is stressed that all actions on the microcircuits during maintenance need to be carefully monitored. Preventative and corrective maintenance plans for microcircuits should take into account that components may be damaged or that redundant parts may not be operative. Tests which are capable of damaging microcircuits (e.g. by overloading unprotected parts) should not be undertaken until a reasonable understanding of the status of the electronics is achieved. In this respect ESD damage is the pertinent concern.

Recommendation 12

The AECB should request evidence that maintenance plans are structured to avoid damage to microcircuits, whether complete or partially dismantled, during testing.

3. GUIDELINES TO RELIABILITY ACTIVITIES AT THE LIFE CYCLE STAGES OF MICROCIRCUITS

3.1 System Design Decisions

A general guideline is that known technology be used where possible.

The major system design decision which would affect microcircuits and their contribution to reliability is whether to use central or distributed processing. If distributed processing is chosen, a number of guidelines apply:

(a) The baud rate will determine the degree of protection needed for a multiplex cable to assure a stated reliability. When the expected baud rate is known the cable protector may be chosen.

(b) Where possible, groups of microprocessors should be situated together in waterproof, cooled protected rooms. Where instead they are to be situated within and around working equipment, certain environmental information will

be needed. For retrofit microprocessors it will be obtained through survey, and for new situations and post-LOCA situations, through survey and extrapolation. The information needed is:

- local temperature changes
- local electromagnetic fields
- frequency and amplitudes of mechanical disturbances, especially in the sonic and subsonic range
- short term radiation changes

The disturbing effect of the microprocessors themselves on the environment should also be noted.

(c) Maps of the above information should be used in locating the microprocessors. In addition the effect of planned or ad hoc maintenance, such as removal of shielding, use of test equipment, use of radio communications equipment, electrostatic disturbance, mechanical disturbance, should be taken into account.

(d) In all cases it should be remembered that, as well as causing simple failure, increased heat and nuclear radiation will age the devices and may cause intermittent failures. More ominously, small levels of electromagnetic interference, electrostatic discharge, vibration and humidity may cause 'ghost bytes' i.e., intermittent false data, which is unlikely to be detected in error checking or built-in tests. The closer microprocessors are to other thermal, mechanical and electromechanical machinery and the more they must be disturbed by humans during maintenance, the more likely these ill-effects will be displayed.

(e) Until accurate profiles of all the stressors over space and time are known in an area, no Special Safety System devices employing microcircuits shall be placed in that area. Signals which are needed for action after a LOCA shall not be dependant on microcircuits within the containment area.

(f) Total enclosure, cooling systems, EM shielding, vibration mounting and radiation shielding shall be used where the environment is unacceptable.

(g) While voting systems of redundancy may be more economical than check and switch systems, continuing work on the logic of the reliability assessments of voting systems should be made. Systems should be kept as simple as possible.

(h) Guidelines on the exact location of cables should be given to the installers.

3.2 Design of Microcircuits and Microprocessors

It is appreciated that in the context of CANDU reactors the AECB licensees normally do not affect the design of microcircuits or even microprocessors but buy what is offered on the market. In certain high safety applications, custom microcircuits may however be designed. As the ease of custom designing such devices improves (and so therefore the price drops) this may become increasingly an option. In such a situation we would look to see:

(a) known technology used where possible

(b) measured capability for parameters of microcircuits smaller than tolerance limits

(c) microcircuits designed to withstand 125%, or more, of all expected stress levels

(d) self checking capacity

(e) electrostatic and surge suppressors used

(f) electromagnetic radiation formally minimised by design, elecromagnetic interference immunity maximised

(g) radiation hardened devices used where radiation may be expected and continued service is necessary

(h) estimates of thermal environment given to designers be clearly realistic

(i) estimates of vibration environment given to designers be clearly realistic

3.3 Procurement

Careful procurement of microcircuit devices is a major pillar of reliability in complex systems. This is seen as an area which needs strengthening at the present in CANDU plants. Clear procurement strategies, linked to acceptable risk levels, need to be developed by the licensees. The following may be used as guidelines.

(a) known technology used where possible

(b) where the reliability of the system is specified, redundancy may not be offered as excuse for lack of knowledge of, or confidence in, reliabilities of components

(c) component design limits derated using developed derating guidelines

(d) critical item list developed with expected life of items or reliability over specified period. All items on the list to be procured as components which have been evaluated by another party than the manufacturer or distributor. Evaluators may be the US Military (MIL.STD parts), large volume industrial users, or in house specialists using in-house failure data.

(e) consideration be given to using screened components for very critical items or those expected to see common stressors (e.g., heat.)

(f) corrosion resistant finishes be specified for the boards

3.4 Installation

There are three major dangers to electronic equipment during installation:

(a) mechanical damage due to imposed stresses

(b) incorrect location of cables causing mechanical stress on terminals and electromagnetic pick-up from other cables and equipment

(c) electrostatic discharge

The first two, it is assumed, are presently covered by directives to the installers. The latter should be covered as part of a full ESD control plan developed by the facilities for use at the plants. The plan should be deliverable to the AECB.

3.5 Operation

All those coming in the vicinity of these microcircuits (including visitors, administrative staff, support staff and others) need appropriate training so that they may appreciate that changing the environment may degrade the performance of the microcircuits. Electromagnetic and electrostatic sources should be described to them, together with their possible effects. The effect of heat and water on the microcircuits should also be clear to them. Stressors

which negatively impact all redundant processors (as may happen if processors are sited near to detectors) have safety implications and this needs particular emphasis during the training.

3.6 Maintenance

The greatest dangers are experienced by microcircuits during maintenance. For example, they run the risk of:

(a) being touched and enduring ESD
(b) having contaminants introduced to them
(c) having the power cut-off or re-introduced in an inappropriate manner
(d) being stressed during testing

Maintenance training needs to be thorough and upgraded frequently, particularly as retrofit new technology is introduced. Planned testing schemes should also be reviewed and upgraded from time to time. The maintenance people need appropriate areas and equipment to handle the increasingly delicate equipment. Even if the maintenance is simply the replacement of boards and on-site repair is not attempted, the maintenance area needs strict rules and management enforcement of these rules. The maintenance area requires:

(a) restricted access ESD protected areas

(b) posted reminders of dangers to microcircuits

(c) a high level of cleanliness; enforced good housekeeping and extractor fans

(d) calibrated equipment with an enforced calibration plan

(e) easy failure data collection and trend analysis methods. (possibly computerised).

4. SUMMARY

4.1 Collected Recommendations to the AECB

1. (a) Indicate to licensees that new technology should not be adopted lightly. If adopted, an in-depth rationale showing very strong measures taken to assure reliability should be submitted to the AECB, with particular emphasis on procurement practices.

(b) As new microcircuit technology is adopted, request assurance that those in the use environment are aware that their activities will affect the reliability.

2. (a) Require that reliance not be placed completely on the manufacturer's catalog value of reliability for devices but increased confidence be sought for critical systems by the use of MIL.STD parts, parts endorsed by reputable third parties, in-house history of parts failure or auditing/witnessing of the production by the licensees.

(b) Discussions between the AECB and licensees facilities be initiated concerning the joining of GIDEP and monitoring of the GIDEP Alerts.

3. (a) Request the derating rationale as part of the reliability estimates.

(b) Request a list of critical electronic components expected to degrade with age be drawn up, and a plan be developed for in-service tests to track their performance changes.

4. Expect the level of physical and electrical noise protection given to cables carrying multiplexed signals be explicitly dependent upon the planned baud rate.

5. (a) The use of redundancy should not be allowed to obscure safety concerns over components with low or unknown reliabilities. Efforts should be made to ensure procurement of components whose reliability is known and which enjoy a high degree of confidence

(b) Frequent software initiated built-in tests with failure display should be considered for all standby systems and parts whose failures will not be announced.

(c) Require the logic of the reliability of voting systems to be demonstrated by design groups.

6. (a) Request a full ESD control plan from its licensees. The Plan should stress the occurrence of transient effects and latent failures as well as the direct failures.

(b) Investigate this area in more depth with all deliberate haste

(c) Request expected life times of devices sensitive to and subjected to surges, even when they are protected by suppressors.

7. (a) Require the designers to demonstrate that EM emissions and EMI immunity have been formally considered in the design of custom processors at the board and/or the system levels, as well as the normal coupling EMI considerations

   (b) Surveys of typical EM fields be conducted in the types of areas under new consideration for situating electronic systems (e.g., generating halls, containment areas).

8. (a) Pursue, via licensees or on its own initiative, development of a model or analysis of other accident data to allow prediction of local radiation changes in space and time immediately after a LOCA.

   (b) Until this information is available, licensees should use the assumption that all electronic devices in the containment area are failed immediately after a LOCA.

9. (a) Express a preference to licensees that distributed microprocessors be grouped together in clean, protected, water-proof, temperature controlled and humidity controlled areas away from main thermal sources, or in cooled enclosures.

   (b) Request thermal profiles of locations in which retrofit microprocessors are to be situated.

10. Request that procedures for repair areas emphasise the danger to microcircuits of debris from repair activities or contaminants, including common cleaners.

11. (a) Request that for locations with expected high amplitudes of sonic or subsonic vibrations, (i.e., noisy areas) the protection of all microprocessors be explicitly demonstrated by the licensees.

   (b) Request vibratory profiles of locations in which retrofit microprocessors are to be situated.

12. Request evidence that maintenance plans are structured to avoid damage to microcircuits, whether complete or partially dismantled, during testing.

4.2 Summary of the Recommendation Themes

4.2.1 Priority Listing of Themes

Many of the recommendations offered to the AECB are already implicit in their policies but are restated here in general because of their fundamental importance. These include:

- o use known technology whenever possible
- o distrust manufacturers' performance claims
- o use extensive self-checking

Other recommendations are perhaps less obvious. They may be grouped in five sections in order of priority and, in general, suggest that the AECB request:

1. Action from the licensees, where the Spar team felt some urgency was required (See Paragraph 4.2.2).

2. Information to be compiled on the need for reliability (critical items list) and confidence in the reliability obtained (procurement strategies) (See Paragraph 4.2.3).

3. Rationale of certain decisions, where the Spar team sensed the rationales were not applied objectively (See Paragraph 4.2.4).

4. Surveys of certain parameters in areas where microcircuits may be located (See Paragraph 4.2.5).

5. Future work (See Paragraph 4.2.6).

4.2.2 Recommendations for Urgent Action from Licensees

The top priority here is that the licensees immediately start writing and implementing a electrostatic discharge control plan. The microcircuits in use at the moment are in danger of degradation and intermittent failures as long as simple instructions are presumed to protect them without equipment, significant training programs, vigorous enforcement or suitable equipment.

One of the major components of the ESD control plan will be training and reminders for actions. This leads into the general training needed for personnel on dangers to microcircuits, their consequences and how to avoid them.

No processors which are needed after a LOCA should be planned to be located in

the containment area. If microprocessors are to be distributed, priority should be given to grouping them in protected areas.

4.2.3 Needs and Strategies in Procurement

The trade-off necessary between need for reliability and cost is complicated by some gaps in the information tree. A list of critical items needs to be matched with a clear, written, procurement policy of the licensees which states the level of confidence to be gained by different strategies (e.g. use of in-house data, military parts, various screening techniques) and outlines under which circumstances these strategies may be used. Apparently, neither the lists nor the policies now exist.

4.2.4 Decision Rationales

Certain decisions are made with multiple inputs and trade-offs and do not lend themselves easily to simple guide-lines. In these cases the licensees should submit to the AECB, for each design, their philosophy and priorities in making these decisions. These include derating, voting between processors and testing structures.

4.2.5 Survey Requests

It would appear inevitable that distribution of microprocessors will take place, possibly as retrofits. While Recommendation 9(a) is that AECB express a preference for protected groups of processors, it is realistic to expect pressure for them to be more scattered. This is seen by the Spar team as a dangerous move, especially as there are significant fluctuations of the stressors over space and time in the generating halls, their expected location. As a minimum, surveys of the variations in time and space of stressors will make visible the dangers and adequate steps to protect against them may be expected to follow.

4.2.6 Future Work

The Spar team sees several areas in which the AECB is urged to make itself more knowledgeable. The bibliography of Section 6. may prove a starting place to enable this to be an internal task, or outside contracts may be necessary.

The top priority is understanding the various measures for control of electrostatic discharges so that AECB staff may be able to judge the ESD control plans of the licensees. Luckily this is a fairly mature discipline, even if not yet implemented in general. A number of companies specialise in ESD and may give seminars or advice (at no charge if their products are to be used).

The next area is a deeper understanding of the possible procurement strategies of microciruits and other components and for which types and uses of microcircuits they are appropriate.

Areas which are less well developed theoretically but have a major impact on reliability of the instrumentation and control systems are software reliability and voting systems logic. Neither of these are strictly within the mandate of this report but are too important to ignore. Both are in the process of being developed and it is our recommendation that the AECB conduct, or have conducted, regular literature searches in these areas.

The final future work which the Spar team recommends to the AECB concerns discussions with the licensees on the cost/benefit of joining GIDEP.

5. CONCLUSIONS

This report has considered the hardware reliability of Process and Special Safety (Shutdown) electronic instrumentation and control systems in CANDU nuclear power plants situated in North America, in the present and the near term future. It has been assumed that the instrumentation and control systems will increasingly use advanced microcircuits of smaller size, greater speeds, lower power consumption and greater environmental sensitivities than in the past. The pressure towards distributing the processing devices of the system in the generating halls and containment areas has also been considered.

The report has shown that the microcircuits themselves intrinsically increase the reliability of instrumentation and control systems but that many perturbing factors may degrade that intrinsic reliability. These factors are the environments and activities in the manufacturing, installation, operation and maintenance phases. The degradation possibly introduced at the manufacturing stage may be mitigated by careful procurement, external auditing and collection of failure histories. Mitigation of degradation during the installation, operations and maintenance stages starts first by the designers knowing and accepting the use environment. It continues by the control of the activities of anyone who works with or near the microcircuits, so that they present minimum disturbance to the system. This needs to be supported by training, suitable equipment and managerial concern.

The practice of distributing the microprocessors will increase the possibility of the degrading factors affecting the microprocessors during use, and increase the probability of common mode failures on redundant processors. It will require more care in design and more discipline of use activities if the safety and reliability of the systems are not to be eroded.

6. DATA SOURCES AND REFERENCES

(a) U.S. Military Standards Department of Defense, Washington, D.C. 20360.
A wide range of specifications, testing methods, risk levels and background handbooks are available, with particular emphasis in the electronic area.

(b) MIL-HDBK.217D, January 1982.
"Reliability Prediction of Electronic Equipment".
The well known handbook discusses Parts Stress Analysis and Parts Count method in detail and offers a computer program 'RADC-ORACLE' for use with the Parts Stress Analysis.

(c) VSMF Data Control Sources
International Division, Information Handling Services, (5 Inverness Way East, P.O. Box 1154, Englewood, Co U.S.A. 80150)
This is an information handling service available on microfiche or microfilm which covers Military and Industrial standards, specifications and related information on a weekly updateable basis.

(d) DOD.HDBK 263 2 May 1980.
"Electostatic Discharge Control Handbook for Protection of Electrical and Electronic Parts, Assemblies and Equipment (Excluding Electrically Initiated Explosive Devices)."
This U.S. Military Standard Handbook gives causes and mechanisms of failure for electric and electronic parts when affected by Electrostatic Discharge (ESD). It discusses testing for ESD, setting up of protected areas and operating procedures, design of protection networks and personnel training.

(e) Government-Industry Data Exchange Program
GIDEP Operations Center
Corona, California, 91720, U.S.A.

(f) "Taming EMI in Microprocessor Systems", D. White, K. Atkinson and J. Osburn, IEEE Spectrum, pp. 30-37, December 1985.
A detailed paper on causes and solutions to EMI in microprocessors.

(g) "Electronic Equipment Reliability Data", (EERD.2) (1986). Published by Reliability Analysis Center, RADC (RAC) Griffins AFB, NY 13661-5700.
The Reliability Analysis Center is a U.S. Department of Defense Information Analysis Center. EERD 2 provides life cycle reliability data on Military Electronic equipment at the set, group and unit levels. Its purpose is to evaluate common reliability practices and to investigate the relationships between these parameters designed to assist in the development of reliable equipments.

(h) What happens to Semiconductors in a Nuclear Environment?, by D. Myers, pp.131-133; Electronics, March 1978.
Short article on failure mechanisms and sensitivities of semiconductor devices to nuclear radiation. Although old, it is still relevant.

(i) "The Byzantine Generals Problem" by L. Lamport, R. Shostak and M. Pease, ACM Trans. Program, Lang. Sys. Vol.4, pp.382-401, July 1982.
This is the original paper on Byzantine Agreement in Voting Logic systems.